CLAIM AMENDMENTS

The following is a complete listing of the pending claims:

Claims 1 -13. (cancelled)

14. (original) A system, comprising:

a host system, the host system configured to request for file system objects stored by a storage device by identifying the block addresses containing a requested file system object and requesting the storage device to return the content stored at the identified block addresses, the host system being further configured to identify the file system object to the storage device if the requested file system object comprises secure content; and

a storage device having:

a storage medium configured to store security metadata for the secure file system objects; and

a storage engine, the storage engine being configured to respond to block-level requests from the host system by retrieving the content stored at the requested block addresses from the storage medium, the storage engine being further configured to access the security metadata if the block-level requests correspond to content comprising a secure file system object.

15. (original) The system of claim 14, wherein the security metadata includes a locking indicator, the storage engine being configured to prevent access to the

corresponding file system object content if the locking indicator indicates the file system object is locked.

16. (original) The system of claim 15, wherein the storage engine is configured to change the security metadata for a secure file system object in response to an Internet transaction with a validated host system.

17. (original) The system of claim 14, wherein the security metadata includes a play flag, the play flag indicating how many times the corresponding file system object may be played by the host system, the storage engine being configured to prevent access to the corresponding file system object if the play flag indicates that the host system has no remaining play rights.

18. (original) The system of claim 17, wherein the storage engine is configured to erase the security metadata if the play flag indicates that the host system has no remaining play rights.

19. (original) The system of claim 17, wherein the security metadata includes a locking indicator, the storage engine being configured to prevent access to the corresponding file system object content if the locking indicator indicates the file system object is locked, and wherein the storage engine is configured to assert the locking indicator if the play flag indicates that the host system has no remaining play rights.

20. (original) The system of claim 14, wherein the security metadata includes a copy flag, the copy flag indicating how many times the host system may copy the corresponding file system object, the storage engine being configured to prevent access to the corresponding file system object if the copy flag indicates that the host system has no remaining copy rights.

21. (original) The system of claim 20, wherein the storage engine is configured to modify security metadata for a secure file system object through an Internet transaction with an authorized host system.

22. (original) The system of claim 14, wherein the storage engine is configured to generate a secure session key, the storage engine generating the security metadata for each secure file system object by receiving a corresponding encrypted content key from the host system, wherein the content key has been encrypted by the host system using the secure session key, the storage engine being further configured to decrypt the encrypted content key using the secure session key and to encrypt the decrypted content key with a first storage engine encryption key and to write the storage-engine-encrypted content key to the storage medium.

23. (original) A system, comprising:

a host system, the host system being configured to request for non-secure file system objects by identifying the block addresses corresponding to the non-secure file system object and to request for secure file system objects by identifying the file system object; and

a storage device having:

a storage medium configured to store security metadata for the secure file system objects; and

a storage engine, wherein the storage engine is configured to control the file system used to store secure and non-secure file system objects on the storage medium, the storage engine being further configured to respond to block-level requests for non-secure file system objects by translating the block-level requests from the host system to byte-level offsets within a file system object on the storage medium, the storage engine being further configured to control the file system associated with secure file system objects by determining where secure file system objects will be stored on the storage medium and where the corresponding security metadata will be stored on the storage medium.

24. (original) The system of claim 23, wherein the storage engine is a hard disc storage engine and wherein the storage media is a hard disc.

25. (original) The block-level storage device of claim 24, wherein the storage media is a removable hard disc.

26. (original) The system of claim 23, wherein the security metadata includes a locking indicator, the storage engine being configured to prevent access to the corresponding file system object content if the locking indicator indicates the file system object is locked.

27. (original) The system of claim 23, wherein the security metadata includes a play flag, the play flag indicating how many times the corresponding file system object may be played by the host system, the storage engine being configured to prevent access to the corresponding file system object if the play flag indicates that the host system has no remaining play rights.

28. (original) The system of claim 23, wherein the security metadata includes a copy flag, the copy flag indicating how many times the host system may copy the corresponding file system object, the storage engine being configured to prevent access to the corresponding file system object if the copy flag indicates that the host system has no remaining copy rights.

29. (cancelled)

30. (cancelled)

31. (cancelled)